Sector 8 Policy Input for the NERC Board of Trustees & Member Representatives Committee

May 8-9, 2019 Meetings in St. Louis, Missouri

ELCON, on behalf of Large End-Use Consumers, submits the following policy input for the consideration of NERC's Board of Trustees (BOT) and the Member Representatives Committee (MRC). It responds to BOT Chairman Roy Thilly's April 2, 2019 letter to Greg Ford, Chair of the MRC.

SUMMARY

- **Comments on Report Recommendations and Board Actions** — Large Consumers support recommendations that only EACS be included and not monitoring, alarming, and logging systems. A Section 1600 data request and other information gathering actions should have the intention of enhancing voluntary actions and better gauging obstacles to adoption of best practices, plus the cost considerations of changing practices. This would inform next steps on considering modifications to standards, such as better accounting of costs and expected benefits, as well as the efficacy of improved guidance. The Board should emphasize accounting for costs and expected benefits in considering mandatory requirements for low impact systems and recognize that mandatory requirements are unnecessary where the incentives of vendors and low impact entities are aligned with BES security.

- **Additional Actions and Recommendations Regarding Supply Chain Risks** — NERC staff and the Board should continue a risk-based approach for supply chain standards with an emphasize on cost-risk balance. NERC should explore tools to motivate voluntary improvements by helping entities make better risk-informed decisions and differentiate requirements for entities with only low impact BES systems from those with high and medium impact systems. NERC should work with industry to explore opportunities to streamline the verification process for EACMS, protect procurement flexibility, and promote information sharing.

Report Content, Recommendations, and Board Actions

In the draft report, NERC Staff recommends revising the Supply Chain Standards to address Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems, excluding monitoring, alarming, and logging. Large Consumers appreciate the recognition of differentiated treatment for EACMS based on risk level: namely that electronic access controls present a higher risk than monitoring and logging systems. Large Consumers support the recommendations that only EACS be included and not monitoring, alarming, and logging systems.

The report recommends that NERC work with the Critical Infrastructure Protection Committee Supply Chain Working Group to develop guidelines for entities applying supply chain risk management plans to low impact BES Cyber Systems and Protected Cyber Assets (PCAs). It also recommends guidelines for evaluating PCAs on a case-by-case basis to determine if additional supply chain protections are appropriate. The report recommends that entities refer to industry practices and guidelines when developing their CIP-013-1 processes for BES Cyber Systems procurement.

Large Consumers support guidelines that help facilitate better voluntary decisions, especially as an alternative to prescriptive management of supply and transport arrangements. Incorporating feedback from entities will improve the quality of guidelines development and motivate useful alterations. Entities may have good reason to not follow prescriptive industry practices and guidelines that do not reflect the variation in business arrangements and risk profiles across entities. Promoting information sharing and protecting procurement flexibility will keep costs down while motivating innovation in best practices.

The report recommends gathering information on low impact BES Cyber Systems that have External Routable Connectivity to understand their pervasiveness and potential need for standard enhancements. Specifically, the report focuses on two data gathering approaches:

(i) Data requests under Section 1600 of the NERC Rules of Procedure.
(ii) Monitoring of CIP Reliability Standards criteria that differentiate medium from low impact BES Cyber Systems via pre-audit surveys and questionnaires.

Large Consumers appreciate the recognition that low-impact BES Cyber Systems pose a low risk to the reliability of the BES and support the recommendation that low-impact BES Cyber Systems should not be included in the Supply Chain Standards. The report gives appropriate consideration

to the impact framework as it currently exists in the CIP suite of standards. Large Consumers underscore the report's recognition that risk is mitigated as organizations with medium and high impact systems implement supply chain standards across their fleet that includes low-impact BES Cyber Systems. The report correctly notes that risk is further mitigated by supply chain vendors who implement supply chain standards across their systems, not knowing whether they will reside in low, medium or high impact systems.

The report states that NERC will develop an expedited Section 1600 data request to inform whether low impact systems should be included within CIP-013. This is a suitable mechanism for this task, but NERC should develop the instrument with the intention of gathering information to encourage better voluntary actions. Further, this effort should aim to not only evaluate current practices, but also gauge obstacles to adoption of best practices and the cost considerations of changing practices. This would inform next steps on considering modifications to standards affecting low impact systems, such as better accounting of costs and expected benefits, as well as the efficacy of improved guidance and information sharing to improve voluntary practices in lieu of mandatory standards.

The Board should note that perceived deficiencies that surveys, questionnaires, or data requests may reveal do not necessarily require modifications to mandatory standards. Doing so may be counterproductive – given the rapid pace that cyber threats and best practices evolve – or, at least, may impose excessive costs or restrictions on operations and procurement flexibility. Large Consumers strongly recommend that the Board emphasize accounting for costs and expected benefits in considering mandatory requirements for low impact systems and recognize that mandatory requirements are unnecessary where the incentives of vendors and low impact entities are aligned with BES security.

Additional Actions and Recommendations Regarding Supply Chain Risks

Large Consumers advise NERC staff and the Board to keep the following in mind for next steps regarding supply chain risks:

- *Continue a risk-based approach for standards and emphasize a cost-risk balance appreciation*. Large Consumers place a particularly high value on electric reliability and appreciate NERC's diligence in evaluating the risks to Bulk Electric System (BES) security. Large Consumers are also very sensitive to cost impacts. NERC should ensure that any supply chain policies have demonstrated risk-reduction benefits that outweigh costs and evaluate whether more cost-effective alternatives exist.
- *Allow time for existing standards to be implemented*. Accurate evaluation of standards and associated processes can only occur after full implementation.

- *Draw a clear policy distinction between entities with only low impact BES cyber systems and those that have medium and high impact systems.* For example, large industrial consumers generally contain only low impact systems and thus present a categorically lower BES risk profile. Differentiating policy treatment for low impact entities as compared to entities with high and medium systems is consistent with the report findings.
- *Explore tools to motivate voluntary improvements by helping entities make better risk-informed decisions tailored to their unique circumstances*. Low-impact entities are highly motivated to maintain strong internal measures for supply chain and cyber-security protections, which may be enhanced via additional information. For example, better information on common mode vulnerabilities may encourage more diverse and effective practices than uniform requirements. Additional information collection efforts should be done in mind with enhancing voluntary actions by entities with low-impact BES Cyber Systems, as their incentives align with BES security.
- *NERC should work with industry to explore opportunities to streamline the verification process for EACMS, protect procurement flexibility, and promote information sharing*. Industry flexibility in application and implementation over prescriptive standards.

###